Notice of Allowability	Application No.	Applicant(s)	
	10/020,308	YAMAMICHI ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendement filed on 08/12/2006*.

2. ☒ The allowed claim(s) is/are *1-6 and 12-29*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

DETAILED ACTION

1. This is in reply to an amendment after a non-final rejection filed **on August 12, 2006**. Claims **7-11 have been canceled previously**. **Thus claims 1-6 and 12-19** are pending/examined.

2. In the previous office action Examiner allowed **claims 1-6 and 12-15 and 17-19** but rejected indepenent **claim 16** under 35 USC § 101. Applicant has amended **independent claim 16** and overcomes the 35 USC § 101 rejection set forth in the previous office action. Thus the rejection is withdrawn.

Allowable Subject Matter

3. **Claims 1-6 and 12-19** are allowed.

4. The following is an examiner's statement of reasons for allowance:

5. **Claims 1-6 and 12-19 are allowed for** the following reasons.

Regarding, independent claims 1 and 15-18, the reference on the record namely, Dia, discloses some of the limitation of the independent claims 1 and 15-18 as shown below.

Dia discloses a

- **Cryptocommunication system including a transmission apparatus and a reception apparatus wherein,** [figure 1 and 3, ref. "Encoder" and " Decoder"]
- **Said transmission apparatus** [Encoder, shown on figure 3 and figure 1] **is operable to encrypt plaintext to generate ciphertext, perform a one-way operation on the plaintext to generate a first value, and transmit the ciphertext and the first value to said reception apparatus,** [figure 3, ref. "104", ref. Num "106" and ref. Num "108"] (The first value is met to be h2 (x, M) which is generated by performing a one-way hash function on the plain text M,

and the ciphertext is met to be C shown on figure 3, ref. Num "106" which is the result of the plaintext after it is encrypted.)

- **Said reception apparatus is operable to receive the ciphertext and the first value, decrypt the ciphertext to generate decrypted text,[figure 3, ref. Num "112"] perform the one-way operation on the decrypted text to generate a second value,**[figure 3, ref. Num 114, see h2' (x, M)] and
- **Judge that Pull the decrypted text matches the plaintext when the second value and the first value match,** [figure 3. ref. Num "114", see comparing the second hash value with the first hash value]
- **Said transmission apparatus comprises**: [figure 1 and 3, reference "Encoder"]
- **First generating means for generating first additional information;** [Column 2, lines 31-47; figure 3, ref. Num "V"] (The ciphertext C has , a value V and a value W and the first additional information is met to be "X").
- **First operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information; encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext;** [column 2, lines 31-47 and column 2, lines 48-50; Figure 3, ref. Num "102" see "cipehertext"] and

Transmitting means for transmitting the ciphertext, [Figure 3, ref. Num "106" and figure 1, ref. Num "26"] and

Said reception apparatus comprising: [Figure 3, reference "Decoder" and figure 1, ref. Num "24"]

- **Receiving means for receiving the ciphertext transmitted from said transmitting means;** [figure 3, ref. Num "108" see "C"]

- **Second generating means for generating second additional information which is identical to the first additional information generated by said first generating means**; [Figure 3, ref. Num "110"]
- **Decrypting means for decrypting the ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm so as to generate decrypted connected information; and second operation means for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.** [Column 2, lines 53-63]

However, as applicant persuasively argued on the amendment filed on 05/15/2006, the reference on the record does not teach, some of the limitation of the independent claims. In particular, a transmission apparatus operable to encrypt plaintext to generate cipher text, perform a one-way operation on the plaintext to generate a first value, and transmit the cipher text and the first value, said transmission apparatus comprising:

First generating means for generating first additional information;

First operation means for performing **an invertible bit-connecting operation on the plaintext and the first additional information to generate connected information;**

Encrypting means for encrypting the connected information according to the encryption algorithm so as to generate cipher text; and

Transmitting means for transmitting the cipher text.

None of the prior art of record taken singularly of in combination teaches or suggests transmission apparatus containing the above particular functional limitation with the rest of the limitation recited in the respective independent claims. For this reason, independent claims **1 and 15-18** are allowed.

6. The dependent claims which are dependent on the above corresponding **independent claims 1 and 15-18** being further limiting to the independent claim, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
08/18/2006

KAMBIZ ZAND
PRIMARY EXAMINER